Finite Fields and Their Applications **5,** 240–245 (1999)
Article ID ffta.1999.0253, available online at http://www.idealibrary.com on IDEAL®

A Counterexample to Perret's Conjecture on Infinite Class Field Towers for Global Function Fields

Harald Niederreiter

Institute of Discrete Mathematics, Austrian Academy of Sciences, Sonnenfelsgasse 19, A-1010 Vienna, Austria
E-mail: niederreiter@oeaw.ac.at

and

Chaoping Xing

Department of Mathematics, The National University of Singapore, Lower Kent Ridge Road, Singapore 119260
E-mail: xingcp@math.nus.edu.sg

Received May 27, 1998; revised February 10, 1999

We show by a counterexample that Perret's conjecture on infinite class field towers for global function fields is wrong, and so Perret's method of infinite ramified class field towers in the asymptotic theory of global function fields with many rational places breaks down. © 1999 Academic Press

1. INTRODUCTION

Let q be an arbitrary prime power and let $K/\mathbb{F}_q$ be a global function field with full constant field $\mathbb{F}_q$; i.e., K is an algebraic function field over the finite field $\mathbb{F}_q$ with $\mathbb{F}_q$ algebraically closed in K. By a *rational place* of K we mean a place of K of degree 1. We write $g(K)$ for the genus of K and $N(K)$ for the number of rational places of K. For fixed $g \geq 0$ and q we put

$$N_q(g) = \max N(K),$$

where the maximum is extended over all global function fields $K/\mathbb{F}_q$ with $g(K) = g$. Equivalently, $N_q(g)$ is the maximum number of $\mathbb{F}_q$-rational points

1071-5797/99 $30.00

that a smooth, projective, absolutely irreducible algebraic curve over $\mathbb{F}_q$ of given genus g can have.

The asymptotic theory of global function fields with many rational places is concerned with the behavior of $N_q(g)$ for fixed q and $g \to \infty$. The basic quantity in this theory is

$$A(q) = \limsup_{g \to \infty} \frac{N_q(g)}{g},$$

where g runs through positive values. Lower bounds for $A(q)$ are of great interest in applications to algebraic-geometry codes. We refer to the books of Stichtenoth [7] and Tsfasman and Vlădut [8] for known facts about $A(q)$ and their applications to algebraic-geometry codes; for very recent work see [5].

Perret [6] described a method of obtaining lower bounds for $A(q)$ which is based on infinite ramified class field towers for global function fields. However, this method depends on a conjecture which would provide a sufficient condition for the infinitude of certain ramified class field towers. In this note we show by a counterexample that this conjecture is wrong. Before we can state Perret's conjecture, we need further notation and terminology.

Let $K/\mathbb{F}_q$ be a global function field, let D be a positive divisor of K, and let S be a nonempty set of rational places of K with S disjoint from the support $\mathrm{supp}(D)$ of D. For a given prime l, the (l, D, S)-*class field* K_1 of K is the maximal abelian extension of K (in a fixed separable closure of K) with a Galois group of exponent 1 or l such that the global conductor of K_1/K divides D and all places in S split completely in K_1/K. If

$$D = \sum_{P \in \mathrm{supp}(D)} m_P P$$

with positive integers m_P, then we define the positive divisor D_1 of K_1 by

$$D_1 = \sum_{P \in \mathrm{supp}(D)} \sum_{Q|P} m_P Q.$$

We let S_1 be the set of all places of K_1 lying over those in S. Now we iterate the construction above by letting K_2 be the (l, D_1, S_1)-class field of K_1, and so on. In this way we obtain the tower

$$K = K_0 \subseteq K_1 \subseteq K_2 \subseteq \ \dots,$$

which is called the (l, D, S)-*class field tower* of K. This tower is called *infinite* if $K_n \neq K_{n+1}$ for all $n \geq 0$.

For an abelian group G we write $d_l G$ for the l-rank of G. The following conjecture was stated in [6, Conjecture 1].

Perret's Conjecture. If

$$d_l G + |S| \leq \tfrac{1}{4}(d_l G)^2$$

with $G = \mathrm{Gal}(K_1/K)$, then the (l, D, S)-class field tower of K is infinite.

2. THE COUNTEREXAMPLE

First we note the following lower bound for $A(q)$ which can be easily derived from [6] and is independent of Perret's conjecture.

LEMMA 1. *Let $K/\mathbb{F}_q$ be a global function field with $g(K) > 1$, let p be the characteristic of $\mathbb{F}_q$, and let D be a positive divisor of K whose support consists of a single place. If the (p, D, S)-class field tower of K is infinite for some nonempty set S of rational places of K with S disjoint from* $\mathrm{supp}(D)$, *then*

$$A(q) \geq \frac{2|S|}{2g(K) + \deg(D) - 2}.$$

Proof. The degree of the different $\mathrm{Diff}(K_n/K)$ of the extension K_n/K satisfies

$$\deg(\mathrm{Diff}(K_n/K)) \leq ([K_n : K] - 1)\deg(D)$$

by [6, Théorème 1 and Proposition 4]. Therefore the Hurwitz genus formula yields

$$\begin{aligned} 2g(K_n) - 2 &= [K_n : K](2g(K) - 2) + \deg(\mathrm{Diff}(K_n/K)) \\ &\leq [K_n : K](2g(K) + \deg(D) - 2) - \deg(D). \end{aligned}$$

Hence we get

$$\begin{aligned} A(q) &\geq \limsup_{n\to\infty} \frac{2N(K_n)}{2g(K_n)} \\ &\geq \lim_{n\to\infty} \frac{2|S|[K_n : K]}{[K_n : K](2g(K) + \deg(D) - 2) - \deg(D) + 2} \\ &= \frac{2|S|}{2g(K) + \deg(D) - 2}. \end{aligned}$$

∎

Our construction of a counterexample to Perret's conjecture is based on the theory of narrow ray class fields; see [1, Chap. 7; 2] for expositions of this theory. Let $K/\mathbb{F}_q$ be a global function field with $N(K) \geq 1$ and distinguish a rational place ∞ of K. Let A be the ring of elements of K that are regular outside ∞. The *Hilbert class field* H_A is the maximal unramified abelian extension of K (in a fixed separable closure of K) in which ∞ splits completely. Let M be a nonzero integral ideal of A and $\Lambda(M)$ the corresponding M-torsion module stemming from the action of a sign-normalized Drinfeld A-module of rank 1 defined over H_A. Then $E_M = H_A(\Lambda(M))$ is the *narrow ray class field over K with modulus M*.

Now we take $q = 2$ and we consider specifically a global function field $K/\mathbb{F}_2$ with $g(K) = 6$ and $N(K) = 10$. The following explicit example of such a function field is given in [3, Example 6]: $K = \mathbb{F}_2(x, y_1, y_2)$ with

$$y_1^2 + y_1 = x^3 + x, \quad y_2^2 + y_2 = \frac{x^2(x+1)((x+1)y_1 + x^3)}{x^5 + x^4 + x^3 + x^2 + 1}.$$

Distinguish a rational place ∞ of K and let the ring A be as above. According to [10, Lemma 8] there exists a place of K of degree $m \geq 2$ as soon as

$$2^m - 12 \cdot 2^{m/2} > \sum_k (2^k + 12 \cdot 2^{k/2}),$$

where the sum is over all positive divisors k of m with $k < m$. It is easily checked that this condition is satisfied for $m = 18$, and so there exists a place P of K of degree 18. Now let E_M be the narrow ray class field over K with modulus $M = P^2$. Note that the place ∞ splits completely in E_M/K by the theory of narrow ray class extensions. Furthermore, we have

$$d_2\mathrm{Gal}(E_M/K) \geq d_2\mathrm{Gal}(E_M/H_A) = d_2(A/M)^* = 18,$$

where the last identity follows as in the proof of [4, Theorem 3]; that is, we note that

$$(A/M)^* = (A/P^2)^* \simeq (\mathbb{F}_{2^{18}}[t]/(t^2))^*$$

and that the 2-Sylow subgroup of the last group is the direct product of the 18 cyclic subgroups $\langle 1 + \alpha_i t + (t^2) \rangle$, $1 \leq i \leq 18$, where $\alpha_1, \ldots, \alpha_{18}$ form a basis of $\mathbb{F}_{2^{18}}$ over $\mathbb{F}_2$.

Since a subgroup of $\mathrm{Gal}(E_M/K)$ generated by 9 Artin symbols has 2-rank at most 9, it follows that there exists a subfield L of E_M/K such that all 10

rational places of K split completely in L/K and $\mathrm{Gal}(L/K) \simeq (\mathbf{Z}/2\mathbf{Z})^9$. Next we need the following result.

LEMMA 2. *With the notation above, the global conductor of L/K divides $2P$.*

Proof. By the theory of narrow ray class extensions, P is the only possible ramified place in L/K. Thus, by [6, Proposition 1] it remains to show that $|G_2| = 1$, where G_i is the ith ramification group of P in L/K. Let d be the different exponent and e the ramification index of P in L/K and let a be the least integer $k \geq 0$ such that $|G_i| = 1$ for all $i \geq k$. From [5, Lemmas 1 and 2] we deduce that

$$c := \frac{d+a}{e} \leq 2.$$

Note that $e = 2^r$ with $0 \leq r \leq 9$. If $r = 0$, then P is unramified in L/K, and so already $|G_0| = 1$. If $r \geq 1$, then $|G_0| = |G_1| = 2^r$ by ramification theory. If we had $|G_2| > 1$, then the Hilbert different formula shows that

$$d > (2^r - 1) + (2^r - 1) = 2^{r+1} - 2.$$

Also $a \geq 3$, and so

$$c = \frac{d+a}{e} > \frac{2^{r+1}+1}{2^r} > 2,$$

which is a contradiction. ■

Altogether, it follows that if S is the set of all 10 rational places of K and if K_1 is the $(2, 2P, S)$-class field of K, then $L \subseteq K_1$. This implies that

$$d_2\mathrm{Gal}(K_1/K) \geq d_2\mathrm{Gal}(L/K) = 9,$$

and so the condition in Perret's conjecture is satisfied. Hence the validity of this conjecture would imply that the $(2, 2P, S)$-class field tower of K is infinite. But then Lemma 1 would yield

$$A(2) \geq \frac{2|S|}{2g(K) + \deg(2P) - 2} = \frac{10}{23} > \sqrt{2} - 1.$$

This contradicts the well-known bound $A(q) \leq \sqrt{q} - 1$ for all q due to Vlăduț and Drinfeld [9].

This counterexample demonstrates that Perret's conjecture is not valid in general. Consequently, Conjecture 1′ in [6] is also wrong and the lower bounds for $A(q)$ in [6, Sect. III] remain unproved.

REFERENCES

1. D. Goss, "Basic Structures of Function Field Arithmetic," Springer-Verlag, Berlin, 1996.
2. D. R. Hayes, A brief introduction to Drinfeld modules, *in* "The Arithmetic of Function Fields" (D. Goss, D. R. Hayes, and M. I. Rosen, Eds.), pp. 1–32, de Gruyter, Berlin, 1992.
3. H. Niederreiter and C. P. Xing, Explicit global function fields over the binary field with many rational places, *Acta Arith.* **75** (1996), 383–396.
4. H. Niederreiter and C. P. Xing, Drinfeld modules of rank 1 and algebraic curves with many rational points II, *Acta Arith.* **81** (1997), 81–100.
5. H. Niederreiter and C. P. Xing, Global function fields with many rational places and their applications, *in* "Finite Fields: Theory, Applications, and Algorithms" (R. C. Mullin and G. L. Mullen, Eds.), Contemporary Math., Vol. 225, pp. 87–111, Amer. Math. Society, Providence, RI, 1999.
6. M. Perret, Tours ramifiées infinies de corps de classes, *J. Number Theory* **38** (1991), 300–322.
7. H. Stichtenoth, "Algebraic Function Fields and Codes," Springer-Verlag, Berlin, 1993.
8. M. A. Tsfasman and S. G. Vlădut, "Algebraic–Geometric Codes," Kluwer, Dordrecht, 1991.
9. S. G. Vlădut and V. G. Drinfeld, Number of points of an algebraic curve, *Funct. Anal. Appl.* **17** (1983), 53–54.
10. C. P. Xing and H. Niederreiter, Drinfeld modules of rank 1 and algebraic curves with many rational points, *Monatsh. Math.* **127** (1999), 219–241.